# Switch 設備如何設定應用 IP Source Guard

### 需求說明:

對於企業或校園等機關團體,資料保密性相當重要,為了不讓使用者私帶個人電腦接上內 部網路進行資料下載、上網,或是私接寬頻路由器(IP 分享器)以致影響正常網路運作。一般防 制作法除了搭配認證設備對欲進行網路使用的使用者進行複雜的身分驗證外,另外也可簡易透 過 Switch 設備中關於 IP Source Guard (IP/MAC Binding)此功能來達到,此文件範例將教導 各位如何進行相關設定及驗證測試。

### 範例架構拓墣圖:



#### www.zyxel.com.tw

## **ZyXEL**

附註1: 設定此功能時建議請使用交換器 Management(MGMT) Port 來進行設定,以避免啟用 ARP Inspection 功能後即無法控管該交換器。而欲使用 MGMT Port 對交換器進行設定,請將設定交換器用的電腦 IP 設定成 192.168.0.X/24,2 < X < 254

附註 2: IP Source Guard 功能由兩部分所組成,其一為 DHCP Snooping 或 Static Binding (此功能作用為建立一合法網路設備清單,在此清單上的網路設備才可正常的使用網路,否則一 律視為非法設備無法使用),其二為 ARP Inspection(此功能作用為依照前者的合法清單內容, 放行或拒絕由交換器所偵測到的 ARP 封包)。

附註 3: 關於 DHCP snooping 此功能設定, 觀念步驟如下:

- Step1. 啟動 DHCP snooping 此功能
- Step 2. 在 Switch 內每個 VLAN 設定中, 啟動 DHCP snooping 此功能
- Step 3. 規劃設定 trusted 以及 untrusted ports
- Step 4. 依需求決定是否新增設定 static bindings.
- 附註 4: 關於 ARP inspection 此功能設定, 觀念步驟如下:
- Step 1 首先設定完成 DHCP snooping 相關功能
- Step 2 在 Switch 內每個 VLAN 設定中, 啟動 ARP inspection 此功能
- Step 3 規劃設定 trusted 以及 untrusted ports.

## 交換器設定說明:

第一部分: DHCP Snooping 或 Static Binding 設定

(1)For dynamic IP(動態 IP 位址綁定)設定如下步驟:

步驟1:在 Advanced Application > IP Source Guard 此頁面點選,點選 DHCP Snooping

	ZyXEL							
	MENU Basic Setting		P Source Guard		Static Binding	DHCP Snoo	ping ARI	<sup>o</sup> Inspection
	Advanced Application				58. Carriero e de la companya <del>-</del> s	21 DE TREAT & LESS NO.000		
	IP Application	Index	MAC Address	IP Address	Lease	Туре	VID	Port
3		2						
2	wanagement	X						
2								
2	VLAN							
	Static MAC Forwarding							
	Filtering							
	Spanning Tree Protocol							
	Bandwidth Control							
	Broadcast Storm Control							
	Mirroring							
	Link Aggregation							
	Port Authentication							
	Port Security							
	Classifier							
	Policy Rule							
	Queuing Method							
	VLAN Stacking							
	Multicast							
	Auth and Acct							
	IP Source Guard							
	Loop Guard							

### 步驟 2: 點選 Configure

OHCP Snooping		Configure IPSG
Database Status		4
Description	Statu	15
Agent URL		
Write delay timer	300	seconds
Abort timer	300	seconds

步驟 3:點選 Port,設定 Trust port(這邊範例為由 port20 介接上端 DHCP Sever)



Configure

THE PROHOUTHTEN
-----------------

DHCP Snooping Configure	Port VLAN DHCP Snooping
Active	
DHCP Vlan	Disable

#### OHCP Snooping Port Configure

Port	Server Trusted state	Rate (pps)
	Untrusted -	
1	Untrusted -	0
2	Untrusted -	0
3	Untrusted -	0
20	Trusted 🔫	0
21	Untrusted -	0
22	Untrusted -	0
23	Untrusted -	0
24	Untrusted -	0

Apply	Cancel
-------	--------

### 步驟 4: 切換回主頁面,點選 VLAN (這邊範例為將 VLAN1 設為 Yes 啟動)

Show VLAN	Start VID	End VI	D
	A	pply	
		and the states	12 10 20 10 10 10 20 20
VID	Enabled	Option82	Informatio
VID *	Enabled No -	Option82	Informatio
VID * 1	Enabled No - Yes -	Option82	
VID * 1 2	Enabled No - Yes - No -	Option82	

步驟 5: 切換回主頁面,將此功能打勾 Active,另外關於 Database 設定欄位建議也需要設定,



請於網路環境中架設一台 DHCP Snooping database server(TFTP Server) 來儲存動態的

dynamic binding table,否則若交換器有手動重開機狀況發生,則動態 dynamic binding

table 將會被清除,請注意!交換器只會保留靜態 static binding table!

COD DHCP Snooping Configure		Port	VLAN	DHCP Snooping
Active	7			
DHCP Vlan	<ul> <li>Disable</li> <li>O</li> </ul>	]		

#### Database

Agent URL	ttp://172.2	4.68.250/dhcp.txt	
Timeout interval	300	seconds	
Write delay interval	300	seconds	
Renew DHCP Snooping URL	ttp://172.2	4.68.250/dhcp.txt	Renew



步驟 6:此時 PC2 電腦網路線重新插拔後,待檢查 Timer 時間到後,即會在選單看到如下所示

的 dynamic binding table · 此代表完成正確設定。(若電腦網卡由 DHCP 方式取得 IP 位址 ·

當成功設定 DHCP Snooping 功能後,則 table 中的 Lease 欄位與 Type 欄位會顯示為

0d9h59m55s 與 dhcp-snooping 此格式。

	P Source Guard	<u>S</u>	tatic Binding	DHCP Snoopin	g <u>ARI</u>	P Inspection
Index	MAC Address	IP Address	Lease	Туре	VID	Port
1	00:c0:9f:9b:c6:f6	172.24.68.73	0d 9h59m55s	dhcp-snooping	1	6

**ZyXEL** 

(2)For Static Binding(靜態 IP 位址綁定)設定如下步驟:

步驟 1: 在 Advanced Application > IP Source Guard 此頁面點選,點選 Static Binding,建

立一筆靜態合法清單內容。

	ZyXEL							
Q	MENU							
3	Basic Setting		P Source Guard		Static Binding	DHCP Snoop	ing ARI	<sup>D</sup> Inspection
ena	Advanced Application	Index	MAC Address	IP Address	Lease	Туре	VID	Port
9	IP Application							
	Management							
5-31								
24	VLAN							
	Static MAC Forwarding							
	Filtering							
	Spanning Tree Protocol							
	Bandwidth Control							
	Broadcast Storm Control							
	Mirroring							
	Link Aggregation							
	Port Authentication							
	Port Security							
	Classifier							
	Policy Rule							
	Queuing Method							
	VLAN Stacking							
	Multicast							
	Auth and Acct							
	IP Source Guard							
	Loop Guard							

步驟 2:在此輸入您准許使用之網路設備 MAC 位址、IP 位址、VLAN 與 Port,最後點選 Add

MAC Address	00	: 1a	: 80	: 3e	: 1f	: b9
IP Address	172.2	4.68.57		<u></u>	rado dando or	
VLAN	1					
	a 2				Barrach Barrach B	

進行新增。

步驟 3: 點選該頁面右上角之 IPSG 回到 IP Source Guard 功能設定頁面,在此即可立刻檢視您

剛設定之 PC1 電腦資料。(若是電腦網卡為 Static IP 位址,故在 Lease 欄位顯示為

inifinity · Type 欄位顯示為 static 此格式。)

IP Source Guard		<u>Sta</u>	atic Binding	DHCP Snooping	ARI	P Inspection
Index	MAC Address	IP Address	Lease	Туре	VID	Port
1	00:1a:80:3e:1f:b9	172.24.68.57	inifinity	static	1	2

依照以下設定範例即完成設備合法清單之設定·接下來需設定 ARP Inspection 功能來過濾合

法與非法的 ARP 封包。

# 第二部分:設定 ARP Inspection

步驟1:點選 ARP Inspection 來達到過濾網路上非法之 ARP 封包。

ZyXEL						۵	Save 🖻 S
MENU Basic Setting		P Source Guard	<u>St</u>	atic Binding	DHCP Snoo	ping ARI	<sup>o</sup> Inspection
Advanced Application IP Application	Index	MAC Address	IP Address	Lease	Туре	VID	Port
Management							
VLAN							
Static MAC Forwarding							
Filtering							
Spanning Tree Protocol							
Bandwidth Control							
Broadcast Storm Control							
Link Aggregation							
Port Authentication							
Port Security							
Classifier							
Policy Rule							
Queuing Method							
VLAN Stacking							
Multicast							
Auth and Acct							
P Source Guard							
Loop Guard							



### 步驟2:點選 Configure 組態相關設定。

ZyXEL							🗉 Save 🖪
MENU		001 00		VIANC			Inco
Basic Setting		RP Inspection St	atus	VLAN S	tatus Log Sta	tus <u>Configu</u>	
Advanced Application	Total nur	nhor of filtors = A					
IP Application	Index	MAC Address	MD	Port	Expiry (sec)	Reason	Delete
Management	*	-	-	-	-	-	
M AN				Delete	Cancel		
Static MAC Forwarding							
Filtering							
Spanning Tree Protocol							
Bandwidth Control							
Broadcast Storm Control							
Mirroring							
Link Aggregation							
Port Authentication							
Port Security							
Classifier							
Policy Rule							
Queuing Method							
VLAN Stacking							
Multicast	Change F	Previo	ue Pana	Nevt Pa	an		
Auth and Acct	change F	ayes	usiaye		90		
IP Source Guard							

### 步驟3:點選 VLAN 好在個別 VLAN 分別啟用 ARP Inspection。

ZyXEL				🗉 Save 🖻 Stati
MENU	ARP Inspection Configure		Port VI AN	APP Inspection
Dasic Setting			TOIL YEAH	Art inspection
Advanced Application				
IP Application	Active			
Management				
	Filter Aging Time			
VLAN	3.3			
Static MAC Forwarding		-		
Filtering	Filter aging time	300	seconds	
Spanning Tree Protocol				
Bandwidth Control				
Broadcast Storm Control				
Mirroring	Log Profile			
Link Aggregation				
Port Authentication				
Port Security	Log buffer size	32	entries	
Classifier	Syslog rate	5	entries	
Policy Rule	l on interval	1	occordo	normanomanomanomanom
Queuing Method	Logintervar	1	seconds	
VLAN Stacking				
Multicast				
Auth and Acct		Apply	Cancel	
IP Source Guard				

步驟 4:在此以 VLAN1 為設定範例。分別在 Start VID 與 End VID 輸入 VLAN 範圍,例如前

後欄位各輸入「1」,然後點選 Apply 進行確認。如圖所示,請在 VID 1 Enabled 欄位

ZyXEL			I	🗉 Save 🖻
MENU Basic Setting	ARP Inspection \	/LAN Configure		Configure
Advanced Application				
P Application	VLAN	Start V/D	End 3/0	1
Management			Line the L	
		Apply		
VLAN		( spbi3		
Static MAC Forwarding				
Filtering	Van	Enabled	Los	
Spanning Tree Protocol	VID	Enableu	LUG	
Bandwidth Control			INone	
Broadcast Storm Control	1	Yes 💌	Deny	2
Mirroring				
Link Aggregation		Annly Cancel	1	
Port Authentication		shbiy cancer	J	
Port Security				
Classifier				
Policy Rule				
Queuing Method				
VLAN Stacking				
Multicast				
Auth and Acct				
IP Source Guard				

點選「Yes」,最後點選 Apply 進行設定值套用即可。

步驟 5:設定完成後,點選此頁面之右上角之 Configure 回到 ARP Inspection

相關設定頁面。

**步驟 6**:點選此頁面之 Port 進行 port 狀態設定。對於 ARP Inspection 功能 · Port 分成兩種 狀態 · 一為信任(Trusted)Port、另一為不信任(Untrusted)Port。ARP 封包「永遠」不會被

ARP Inspection 信任的 Port 所丟棄,但不信任的 Port 之 ARP 封包會被丟棄,前提是該 ARP

Configure

封包的來源 MAC、VLAN 資訊不在合法清單內或在規定時間內所接收到的 ARP 封包頻率超過

合法設定值。依架構拓墣圖說明,在 Port20 設定為 Trusted Port,最後點選 Apply 進行套用。

ARP Inspection Port Configure

Dort	Tructod Stato	Limit		
FOIL	Trusted state	Rate (pps)	Burst interval (seconds)	
*	Untrusted 💌			
1	Untrusted 💌	15	1	
2	Untrusted 💌	15	1	
3	Untrusted 👻	15	1	
19	Untrusted 👻	15	1	
20	Trusted 🔻	15	1	
21	Untrusted 💌	15	1	
22	Untrusted 💌	15	1	
23	Untrusted 💌	15	1	
24	Untrusted 💌	15	1	
25	Untrusted 💌	15	1	
26	Untrusted 👻	15	1	
27	Untrusted 👻	15	1	
28	Untrusted 👻	15	1	

Apply Cancel

步驟7:設定完成後,點選此頁面之右上角之 Configure 回到 ARP Inspection 相關設定頁面。

步骤8:最後勾選Active, 啟用 ARP Inspection 功能, 並點選 Apply 進行套用。



MENU					
Basic Setting	🔹 🤇 🥥 ARP Inspection Configure		Port	VLAN	ARP Inspection
Advanced Application		$\frown$			
P Application	Active	ন			
Management		- Inner I			
	Filter Aging Time				
VLAN					
Static MAC Forwarding		600			
Filtering	Filter aging time	1300	seconds		
Spanning Tree Protocol					
Bandwidth Control					
Broadcast Storm Control					
Mirroring	Log Profile				
Link Aggregation					
Port Authentication		1	_		
Port Security	Log buffer size	32	entries		
Classifier	Syslog rate	5	entries		
Policy Rule	Log interval	1	soconde		
Queuing Method	Log morta	T.	seconds		
VLAN Stacking					
Multicast			28		
Auth and Acct		Apply	Cancel		
IP Source Guard					
Loop Guard					

# 第三部分:測試驗證

www.zyxel.com.tw

先由一部合法網路設備(PC2)成功取得 DHCP Server 配發之 IP · 然後測試可否正常 執行任何網路運作 · 接著由該手動變更網卡 IP 位址 · 其 IP 位址為原本 DHCP pool 範圍內 · 測

試 IP Source Guard 功能是否成功偵測與拒絕該變更過後的非法 IP 位址。

步驟1:將合法網路設備(PC2)串接至ES-3124的Port6·並成功由DHCP Server 取得IP·然後進行網路服務測試·例如:Ping HiNet DNS Server·此時會發現可成功藉由ARP Request 封包得知 Gateway MAC 位址。

網址① 💊 網路連線			
	医域網路或高	速洞際網路	ł
網路工作 📀			
🛐 建立一個新連線		<b>2</b>	<b>Z</b>
💁 設定家用或小型辦公室網路	1394 連線	區域連続	
😂 變更您的 Windows 防火牆設			停用(B)
○ 定値			<b>狀態(U)</b>
	寛頬		修復史
💊 修復這個連線		~ *	橋接器連線(G)
📑 重新命名這個連線		- 22 -	
🕥 檢視這個連線的狀態	200	200	建立捷徑(5)
→ 變更這個連線的設定	TFN	HiNet	刪除(D)
			重新命名( <u>M</u> )
		-	
其他位置 📀		Ļ	11B/(27)
◎ 经制台			

步驟 2:停用 NB 網路卡介面,目的為變更 IP 配置為手動設定。

步驟 3:將 IP 位址由 DHCP 配置變更為手動配置,配置資訊如圖所示,設定完

畢後,請點選**確定**進行設定值套用。

股 ]果您的網路支援這項功能, ],您必須詢問網路系統管理	您可以取得自動指派的 IP 設定。否 員正確的 IP 設定。
○ 自動取得 IP 位址(Q)	
⊙使用下列的 IP 位址(≦):	S
IP 位址①:	172 . 24 . 68 . 215
子網路遮罩(1):	255 . 255 . 255 . 0
預設閘道(D):	172 . 24 . 68 . 254
●自動取得 DNS 伺服器位为 ●使用下列的 DNS 伺服器位 慣用 DNS 伺服器(P):	上田) 江址(国): 168 . 95 . 1 . 1
其他 DNS 伺服器( <u>A</u> ):	<u> </u>

步驟4:重新啟用電腦網路卡介面執行測試。

8世(D) 🛸 網路連線	<b>画域網羅</b>	A或百速洞際洞路	<b>Å</b>
<ul> <li>網路工作</li> <li>■ 建立一個新連線</li> <li>▲ 設定家用或小型辦公</li> </ul>	◎ 2/201/201/201/201/201/201/201/201/201/20		
<ul> <li>              愛更您的 Windows</li></ul>	火牆設		<b>啓用(丛)</b> 狀態(匹)
<ul> <li>重新命名這個連線</li> <li>變更這個連線的設定</li> </ul>	展算 ····································	<b>1</b>	建立捷徑(S) 刪除(D) 重新命名( <u>M</u> )
其他位置	TFN	HiNet	内容(R)
▶ 控制台			

步驟 5:重新執行網路服務測試,例如: Ping HiNet DNS Server,此時會發現無法藉由 ARP Request 封包得知 Gateway MAC 位址,所以封包無法連接網際網路。

步驟 6:另外也可藉由網路封包擷取軟體驗證步驟五,確認為 NB 有發出 ARP Request 封包,但 Gateway 端卻無回應,原因為交換器將其 ARP 封包視為非法之 ARP 封包而丟棄,此部份可由步驟七來進行得知。

**步驟 7**:為查詢得知步驟五之 ARP 封包被交換器所偵測到並視為非法封包與之丟棄,請點選 Advanced Application > IP Source Guard > ARP Inspection > VLAN Status,此頁面請 直接點選 Apply 進行有啟用 ARP Inspection 功能之 VLAN 的狀態觀看。在此可看到被丟棄 的 ARP 封包數截至目前為止共 62 個。



ZyXEL						🗉 Save	🖬 Status
MENU		ation MI ANIS	10110			C4	
Basic Setting	ARE Inspe	CUON VEAN S	tatus			30	atus
Advanced Application							
IP Application	240700447047048000	C Enabled VL	AN				
Management	Show VLAN range	C Selected VI	LAN Sta	rt VID	End VID		
			_				_
VLAN			Ap	ply			
Static MAC Forwarding	-						74
Filtering							
Spanning Tree Protocol							
Bandwidth Control	VID	Received	Request	Reply	Forwarded	Dropped	5
Broadcast Storm Control	1	83	79	4	21	62	
Mirroring							
Link Aggregation	-						
Port Authentication							
Port Security							
Classifier							
Policy Rule							
Queuing Method							
VLAN Stacking							
Multicast							
Auth and Acct							
IP Source Guard							

步驟 8: 切換回 ARP Inspection 頁面,在此頁面您可看到交換器將偵測到的非法 ARP 封包之

來源 MAC 位址、VLAN 與拒絕之理由(即 Reason 欄位)一應俱全加以進行記錄。

Basic Setting	ARP Inspection Status			VLAN St	atus Log Sta	tus <u>Config</u> u	ire IPSC
Advanced Application P Application	Total nun	nber of filters = 1 MAC Address	VID	Port	Expiry (sec)	Reason	Delete
Management	*	-	-	-	-	-	
	1	00:0d:60:cb:fc:ac		6	256	IP	
VLAN							
Static MAC Forwarding				Delete C	ancel		
Filtering							
Spanning Tree Protocol							
Bandwidth Control							
Broadcast Storm Control							
Mirroring							
Link Aggregation							
Port Authentication							
Port Authentication Port Security							
Port Authentication Port Security Classifier							
Port Authentication Port Security Classifier Policy Rule							
Port Authentication Port Security Classifier Policy Rule Queuing Method							
Port Authentication Port Security Classifier Policy Rule Queuing Method VLAN Stacking							

請注意此頁面之 Expire 欄位,預設值為 300 秒,若任何非法日誌清單尚未過期之前,即使

您將原本合法之網路設備變更回原始合法設定值後,也將無法正常運行。例如:以架構範例圖

# **ZyXEL**

#### www.zyxel.com.tw

為例,今交換器上已接上合法電腦可進行使用,但若使用者私帶其他電腦利用相同 Por改串接該私有電腦,則該私有電腦一定無法進行使用,待使用者接回原本合法電腦,此時該合法電腦 亦無法進行使用,原因為私有電腦非法之 ARP 封包已遭受交換器加以記錄,除非待該項日誌到 期後,原本合法電腦才可再次進行任何網路服務使用。

## End of the Document